FGN, algèbre 1
p. 153 - 153

Développement : Théorème de Dirichlet faible :

Leçons 102
120
121
141

Il n'existe aucune formule explicite de type polynomiale pour atteindre tous les nombres premiers, c'est même prouvé. En revanche il en existe une infinité retrouvable grâce à un polynôme de degré 1.

Lemme : Soit $a \in \mathbb{N}$. Soit p premier tq p divise $\varphi_n(a)$ mais $p \nmid \varphi_d(a)$ $\forall d$ diviseur de n, alors $p \equiv 1 \ [n]$.

Preuve :

Dans $\mathbb{Z}$, nous avons $a^n - 1 = \prod_{d|n} \varphi_d(a)$. On $p \mid \varphi_n(a)$ donc $p \mid a^n - 1$, i.e. $a^n \equiv 1 \ [p]$. Nous allons maintenant montrer que $\bar{a}$ est exactement d'ordre n dans $\mathbb{F}_p^*$.

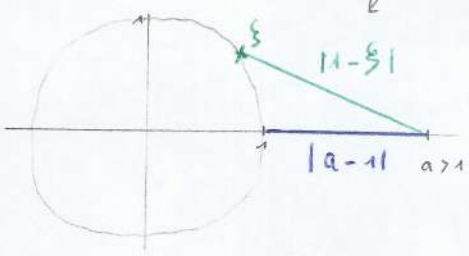
Soit w l'ordre de $\bar{a}$ dans $\mathbb{F}_p^*$. Déjà, $w \mid n$. On, $a^w - 1 = \prod_{d|w} \varphi_d(a)$ et si $w < n$, $\exists$ d diviseur strict de n tq $p \mid \varphi_d(a)$, ce qui est exclus ! Donc $w = n$. Ainsi l'ordre de $\bar{a}$ dans $\mathbb{F}_p^*$ est n, et $\mathbb{F}_p^*$ d'ordre $p-1$. Ainsi $n \mid p-1$, ie $p \equiv 1 \ [n]$. ∎

Théorème : Il existe une infinité de nombres premiers de la forme $\lambda n + 1$, $\lambda \in \mathbb{N}^*$.

Preuve :

Soit $N \in \mathbb{N}^*$ tq $N \geq n$. Posons $a = 3.N!$ (le $N!$ assure que notre nombre a contient tous les nombres premiers jusqu'à N, et le 3 permet d'assurer la propriété suivante)

$\varphi_n(a) \in \mathbb{Z}$ et $|\varphi_n(a)| = \prod_{i=1}^{n} |a - e^{\frac{2ik\pi}{n}}| \geq \prod_{i=1}^{n} |a-1| \geq a - 1 \geq 2$



Soit p un diviseur premier de $\varphi_n(a)$ (existe car $|\varphi_n(a)| \geq 2$)

- Si $p \leq N$, p divise a (par construction de a) donc divise tout entier de la forme $\sum_{i=1}^{n} z_i \cdot a^i$ $(z_i \in \mathbb{Z})$, et donc particulièrement $\varphi_n(a) - \varphi_n(0)$.

  Ainsi $p \mid \varphi_n(0) = \pm 1$: absurde... donc $p > N$.

  $\varphi_n(a) - \varphi_n(0) = \prod_{k=n}^{\hat{}} (a - e^{\frac{2ik\pi}{n}}) - \prod_{k=1}^{\hat{}} (-e^{\frac{2ik\pi}{n}})$
  et en développant, on voit que ceci est $= \sum_{i=1} a_i z^i$

- Soit d diviseur strict de n tq $p \mid \varphi_d(a)$

  $X^n - 1 = \prod_{d \mid n} \varphi_d(X)$ donc $\bar{a}$ est une racine de multiplicité ≥ 2 de $X^n - \bar{1}$ dans $\mathbb{F}_p[X]$ (en effet, $\bar{a}$ racine d'un φ_d et de φ_n). Par conséquent $X^n - \bar{1} \in \mathbb{F}_p[X]$ possède une racine multiple ce qui est absurde car $(X^n - \bar{1}) \wedge (\bar{n} \cdot X^{n-1}) = 1$ (Bézout : $\frac{1}{\bar{n}} \cdot X \cdot \bar{n} \cdot X^{n-1} - (X^n - \bar{1}) = \bar{1}$).

  Ainsi $p \mid \varphi_n(a)$ mais aucun des $\varphi_d(a)$ avec d diviseur strict de n, donc $p \equiv 1 \ [n]$. Ainsi $\forall N \in \mathbb{N}^*$, $\exists$ p premier tq $p > N$ et $p \equiv 1 \ [n]$ - (càd $p = 1 + \lambda \cdot n$, $\lambda \in \mathbb{Z}$).